1.3 带余除法

问题：多项式 +，−，数乘、直接相乘，结果都是多项式。除法呢？ ⟶ 带余除法

Def 1、设 $\mathbb{P}$ 是一个数域，$f(x), g(x) \in \mathbb{P}[x]$. 且 $g(x) \neq 0$.
如果 $q(x), r(x) \in \mathbb{P}[x]$ 满足：

1) $f(x) = g(x)q(x) + r(x)$.
2) $r(x) = 0$ 或 $\deg r(x) < \deg g(x)$.

则称 $q(x)$ 是 $g(x)$ 除 $f(x)$ 的<u>商式</u>，~~$r(x)$ 为~~ $r(x)$ <u>余式</u>.

可以使用大除法计算两个多项式之除法.

Eg 1. 求 x^2-3x+1 除 $3x^3+4x^2-5x+6$ 的商式与余式.

$$
\begin{array}{r@{}l}
 & \quad 3x+13 \quad \longleftarrow \text{商式} \\
x^2-3x+1 \,\big) & \, 3x^3+4x^2-5x+6 \\
 & \, \underline{3x^3-9x^2+3x} \\
 & \qquad 13x^2-8x+6 \\
 & \qquad \underline{13x^2-39x+13} \\
 & \qquad\quad 31x-7 \quad \longleftarrow \text{余式}.
\end{array}
$$

许多时候，我们仅对于一次因式感兴趣. 后续我们看到，任意多项式在 $\mathbb{C}$ 中可以分解成若干一次因式之乘积.

故介绍

<u>综合除法</u>. 如果 $f(x) = \sum_{i=0}^{n} a_i x^i$，$g(x) = x - a$，那么余式 $r \in \mathbb{P}$. 商式 $q(x) = \sum_{j=0}^{n-1} b_j x^j$. 此时有：

$$
\begin{aligned}
b_{n-1} &= a_n \\
b_i &= a b_{i+1} + a_i, \quad \forall i < n-1. \\
r &= a b_0 + a_0
\end{aligned}
$$

简便起见，可使用下表计算 $q(x)$ 各项系数与 r：

$$\begin{array}{c|cccc|c} a & a_n & a_{n-1} & \cdots & a_1 & a_0 \\ \hline & b_{n-1} & b_{n-2} & & b_0 & r \end{array}$$

$b_{n-1}\ b_{n-2}\ \cdots\ b_0$：对应商

r：余式.

Eg 2.(1)求 拿 $x+1$ 除 $x^4-8x^3+x^2+4x-6$ 的商与余式

$$\begin{array}{c|ccccc} -1 & 1 & -8 & 1 & 4 & -6 \\ \hline & 1 & -9 & 10 & -6 & 0. \end{array}$$

$1\times(-1)+(-8)=-9$

意味着余式为0，商式为 $x^3-9x^2+10x-6$.

(2) 求拿 $x-3$ 除 $2x^5-x^4-3x^3+x-3$ 之商与余式.

$$\begin{array}{c|cccccc} 3 & 2 & -1 & -3 & 0 & 1 & -3 \\ \hline & 2 & 5 & 12 & 36 & 109 & 324 \end{array}$$

Th 1、设 $f(x), g(x)\in \mathbb{P}[x]$，且 $g(x)\neq 0$. 则 $f(x)$ 除以 $g(x)$ 的商和余式存在唯一.

Guide:
存在性？
唯一性？

证.（存在性）.

~~首先证~~

1° 如果 $f(x)=0$ 或 $\deg f(x)<\deg g(x)$，则取 $q(x)=0$.
$r(x)=f(x)$.

即 $f(x)=0\cdot g(x)+f(x)$.

$\Rightarrow 0, f(x)$ 分别为商和余式.

2° 余下讨论 $\deg f(x)\geq \deg g(x)$ 的情况. 由于 $\deg f(x)<\deg g(x)$ 的情况已经成立.

使用第二类数学归纳法证明.

设 $f(x)=\sum_{i=0}^{m} a_i x^i$ ，$a_m\neq 0$

$g(x)=\sum_{j=0}^{n} b_j x^j$ ，$b_n\neq 0$ ，$n\leq m$.

令① $f_1(x)=f(x)-g(x)\frac{a_m}{b_n}x^{m-n}$ ，则 $\deg f_1(x)<\deg f(x)$.

想要每一次把系数"凑对"　　干掉最高项，目的.

于是有 $q_1(x), r(x)\in \mathbb{P}[x]$, s.t.

② $\begin{cases} f_1(x)=g(x)q_1(x)+r(x) \\ r(x)=0 \text{ 或 } \deg r(x)<\deg g(x). \end{cases}$　（定义）

~~代入~~

将②式代入①式. $f(x)=g(x)\left(\frac{a_m}{b_n}x^{m-n}+q_1(x)\right)+r(x)$.

显然. $\frac{a_m}{b_n}x^{m-n}+q_1(x)$ 是 商式

$r(x)$ 余式.

（唯一性）. 设（反证法）. $q(x), r(x)$ ；$p(x), s(x)$ 是 $g(x)$ 除 $f(x)$ 商与余式.

因而 $f(x)=g(x)q(x)+r(x)=g(x)p(x)+s(x)$

$\Rightarrow r(x)-s(x)=g(x)(p(x)-q(x))$

若 $p(x)\neq q(x)$ ，由 $g(x)\neq 0$. 故 $r(x)-s(x)\neq 0$.

但是 $\underbrace{\deg(r(x)-s(x))}_{\text{次数小一些.}}<\deg g(x)\leq \deg g(x)(p(x)-q(x))$.　??

$\Rightarrow\Leftarrow$!

因此 $p(x)=q(x)$ ，从而 $r(x)=s(x)$

Def 2、设 $f_1(x)$ ，$f_2(x)$ ，$g(x)\in\mathbb{P}[x]$, 且 $g(x)\neq 0$.

如果 $g(x)$ 除 $f_1(x)$ ，$f_2(x)$ 的余式相同，则称 $f_1(x)$ ，$f_2(x)$ 模 $g(x)$ 同余. 记作

$$f_1(x)\equiv f_2(x)\pmod{g(x)}.$$

否则，称 $f_1(x)$ ，$f_2(x)$ 非同余，记作

$$f_1(x)\not\equiv f_2(x)\pmod{g(x)}.$$

Eg. $x^2-2x+2 \equiv x^2 \pmod{(x-1)}$.

Def 3. 设 $f(x), g(x) \in P[x]$ 且 $g(x) \neq 0$. 若 $g(x)$ 除 $f(x)$ 的余式为 0. 则称 $g(x)$ 可整除 $f(x)$，这时称 $g(x)$ 为 $f(x)$ 的因式，$f(x)$ 为 $g(x)$ 的倍式

记作 $g(x) \mid f(x)$.

这个定义是说：若 $g(x) \mid f(x)$，即存在 $q(x) \in P[x]$，

s.t. $f(x) = g(x)q(x)$.

发现 $g(x)$ 除 0 的余式为 0. 故 $g(x) \mid f(x)$.

$\Rightarrow f(x) \equiv 0 \pmod{g(x)}$.

基本性质：

1° $f_1(x) \equiv f_2(x) \pmod{g(x)} \Leftrightarrow$

$$f_1(x) - f_2(x) \equiv 0 \pmod{g(x)}.$$

证：$\Rightarrow$ 若 $f_1(x) \equiv f_2(x) \pmod{g(x)}$，则有

$$f_i(x) = g(x)q_i(x) + r(x),\ i=1,2.$$

两式相减：$f_1(x) - f_2(x) \equiv 0 \pmod{g(x)}$.

$\Leftarrow$ 若 $f_1 - f_2 \equiv 0 \pmod{g(x)}$，即有

$$f_1(x) - f_2(x) = g(x)q(x).$$

设 $g(x)$ 除 $f_i(x)$ 的商式、余式分别为 $q_i(x), r_i(x)$.

故 $f_1(x) - f_2(x) = g(x)(q_1(x) - q_2(x)) + (r_1(x) - r_2(x))$

即 $g(x)$ 除 $f_1(x) - f_2(x)$ 之余式为 $r_1(x) - r_2(x)$. 为 0.

因而 f_1, f_2 模 g 同余.

2° 设 $f_i(x) \equiv h_i(x) \pmod{g(x)}$，$i=1,2$，

则 $$f_1(x) \pm f_2(x) \equiv h_1(x) \pm h_2(x) \pmod{g(x)}$$

$$f_1(x) f_2(x) \equiv h_1(x) h_2(x) \pmod{g(x)}.$$

证：· 设 $f_i(x)$ 除以 $g(x)$ 余式为 $r_i(x)$，$h_i(x)$ 除以 $g(x)$ … $h_i(x)$.

那 $f_1(x) \pm f_2(x)$ 除以 $g(x)$ 余式为 $r_1(x) \pm r_2(x)$.

$\Rightarrow f_1(x) \pm f_2(x) \equiv h_1(x) \pm h_2(x) \pmod{g(x)}$.

· 由 1°（移项），$f_i(x) - h_i(x) = g(x) q_i(x)$，$i=1,2$.

$$\begin{aligned} & f_1(x) f_2(x) - h_1(x) h_2(x) \\ = & f_1 f_2 \underbrace{- f_1 h_2 + f_1 h_2}_{\text{凑进来}} - h_1 h_2 \end{aligned}$$

$\boxed{\text{为了方便起见 } f_1(x) \text{ 简记为 } f_1}$

$$\begin{aligned} & = f_1 (f_2 - h_2) + h_2 (f_1 - h_1) \\ & = g (f_1 q_2 + h_2 q_1) \end{aligned}$$

有公因式.

由 1° 知，$f_1 f_2 = h_1 h_2 \pmod{g}$.

~~3° ∀~~

使用 1° 2° 使得同余式易于像等式那样操作.

（3° $\forall c \in \mathbb{P}$，$c \neq 0$，$f(x) \in \mathbb{P}[x]$，有 $c \mid f(x)$.）

因为 $f(x) = c \cdot (c^{-1} f(x))$.

4° 设 $f(x), g(x) \in \mathbb{P}[x]$，且 $f(x) \neq 0$，$g(x) \neq 0$，

则 $\big(f(x) \mid g(x),\ g(x) \mid f(x)\big) \Leftrightarrow \big(f(x) = c g(x)\big)$.

证：$\Leftarrow$ $f(x) = c g(x) \Rightarrow g(x) \mid f(x)$.

而 $c \neq 0$，$c \in \mathbb{P}$，$g(x) = c^{-1} f(x)$. $f(x) \mid g(x)$

$\Rightarrow$. 若 $f(x)\mid g(x)$, $g(x)\mid f(x)$.

则 $f(x)=g(x)p(x)$

$g(x)=f(x)q(x)$

$f(x)=f(x)p(x)q(x) \Rightarrow p(x)q(x)=1$.

而 $\deg 1=0$. 故 $\deg p(x)=\deg q(x)=0$.

因而 $p(x)=c\in P$, $c\neq 0$.

5° (2°的~~线性~~组合) 若 $g(x)\mid f_i(x)$, $i=1,2,\cdots,k$.

$\forall u_i(x)\in P[x]$, $i=1,2,\cdots,k$, 都有

$$g(x)\,\Big|\,\sum_{i=1}^{k}\underbrace{u_i(x)}_{\text{任何一个多项式}}f_i(x).$$

证: 由2°: $\sum_{i=1}^{k}u_i(x)f_i(x)\equiv\sum_{i=1}^{k}u_i(x)\,0 \pmod{g(x)}$

$\equiv 0 \pmod{(g(x))}$.

称 $\sum_{i=1}^{k}u_i(x)f_i(x)$ 是 $f_1(x)\cdots f_k(x)$ 的一个组合.

6° (传递性) $f(x),g(x),h(x)\in P[x]$. $g(x)\neq 0$, $h(x)\neq 0$.

若 $h(x)\mid g(x)$, $g(x)\mid f(x)$, 则 $h(x)\mid f(x)$.

证: $g(x)=h(x)q_1(x)$,

$f(x)=g(x)q_2(x)$

$\Rightarrow f(x)=h(x)\big(q_1(x)q_2(x)\big)$.

7° 设 P, $\overline{P}$ 都是数域, 且 $P\subseteq\overline{P}$. 又设 $f(x),g(x)\in P[x]$

$g(x)\neq 0$.

则 $g(x)$除$f(x)$在$P[x]$中商、余式 $q(x)$、$r(x)$ 也是

$g(x)$除 $f(x)$ 在 $\overline{P}[x]$中 ....

因而 在$P[x]$中 $g(x)\mid f(x)$ $\Longleftrightarrow$ $\overline{P}[x]$中 $g(x)\mid f(x)$.

~~意味着~~